

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

JOHNNY RAY WOLFENBARGER,

Defendant.

Case No. 16-CR-00519-LHK-1

**AMENDED ORDER DENYING
DEFENDANT'S MOTIONS TO
SUPPRESS**

Re: Dkt. Nos. 183, 184

This order vacates and supersedes ECF No. 207, which was filed on August 29, 2019.

A federal grand jury indicted Defendant Johnny Ray Wolfenbarger ("Defendant") on one count of attempted production of child pornography, in violation of 18 U.S.C. § 2251(c) and (e); one count of attempted coercion and enticement of minors, in violation of 18 U.S.C. § 2422(b); and one count of receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2). ECF No. 1.

Before the Court are two motions to suppress filed by Defendant. In one, Defendant seeks to suppress evidence seized from Defendant's Yahoo email account on the basis that Yahoo acted as a government agent pursuant to the Fourth Amendment and *United States v. Walther*, 652 F.2d 788 (9th Cir. 1981). In the other, Defendant seeks to suppress all evidence pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). The Court held an evidentiary hearing on July 12, 2019 and July

23, 2019. *See* ECF Nos. 199, 203. Having considered the briefs and declarations, the testimony from the evidentiary hearing, the relevant law, and the record in this case, the Court DENIES both of Defendant’s motions to suppress.

I. BACKGROUND

A. Factual Background

1. Yahoo’s Enforcement of its Terms of Service

Yahoo is an Internet service provider (“ISP”). Although Verizon purchased Yahoo in 2017 and renamed the company Verizon Media, the parties and witnesses all refer to the company as Yahoo. Moreover, many of the events in question occurred before Verizon purchased Yahoo, and the witnesses and exhibits frequently refer to the company as Yahoo rather than Verizon Media. The Court follows suit.

Sean Zadig, Senior Director of Cyber Defense at Verizon Media, has worked at Yahoo since 2014 and testified about Yahoo’s operations. Tr. at 163:19-25. Prior to his current role, Zadig was the team lead for Yahoo’s E-Crime Investigation Team (“ECIT”). Tr. at 165:1-7. Zadig testified that ECIT was formed “to investigate abuse on our user platforms, primarily violations of our terms of service.” *Id.* at 170:16-18. A user must agree to those terms of service (“TOS”) when the user creates a Yahoo account. *Id.* at 172:21-24. Yahoo’s TOS states: “By accessing and using the Yahoo Services, you accept and agree to be bound by the terms and provision [sic] of the TOS.” Ex. Q at 8.

On December 18, 2013, Defendant created the Yahoo user account jrwolfen02. Tr. at 168:23-169:2. Under the TOS in effect on that date, any user creating an account agreed not to transmit unlawful or obscene conduct over Yahoo’s services: “You agree to not use the Yahoo Services to: a. upload, post, email, transmit, or otherwise make available any Content that is unlawful, harmful, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, invasive of another’s privacy, hateful, or racially, ethnically, or otherwise objectionable.” Ex. Q at 10. A user also agreed not to use Yahoo’s services to “harm minors in any way.” *Id.*

When a user registers for certain Yahoo services, such as Yahoo Messenger, the user must

1 agree to terms of service specific to those services. Tr. at 177:11-16. Yahoo Messenger’s
2 additional terms of service (“ATOS”) provide that “the user agrees not to use the services in any
3 unlawful manner, for any unlawful purpose, or in any manner inconsistent with the ATOS or the
4 TOS.” Ex. Q at 25. Accordingly, Zadig testified that Yahoo’s TOS and the Messenger ATOS
5 prohibit child pornography and child sexual abuse materials. Tr. at 180:17-21. Yahoo’s TOS
6 provides that Yahoo may screen content stored in user accounts to “comply with legal process” or
7 “enforce the TOS,” among other reasons. Ex. Q at 11, 19.

8 Zadig offered multiple reasons why Yahoo prohibits child sexual abuse materials on its
9 services. First, Yahoo “seek[s] to create a safe place for our users to engage in online conduct and
10 to communicate with each other, to post and exchange ideas,” but child pornography creates an
11 unsafe environment for Yahoo’s users, especially potential minor users. *Id.* at 182:20-22; 182:23-
12 25. A person as young as 13 years old can create a Yahoo account. *Id.* at 186:6-8.

13 Second, child pornography threatens Yahoo’s advertising revenue stream. *Id.* at 183:1-4.
14 Zadig testified that after Google detected child pornography on several blogs on Tumblr—which
15 Yahoo owns—Google threatened to suspend Tumblr from Google’s AdSense network. *Id.* at
16 184:9-14. In December 2018, Apple also temporarily blocked Tumblr’s app from the Apple App
17 Store “because Apple had detected child pornography on one single blog within the Tumblr
18 ecosystem.” *Id.* at 184:15-20. Both actions posed a significant threat to Yahoo. Without a
19 presence in the App Store, for example, no new mobile user could access Tumblr and view ads on
20 Tumblr. *Id.* at 185:21-25. Yahoo’s investigations of violations of its TOS and attempts to remove
21 child pornography are factors that “allowed Apple to let us relist the Tumblr app on the App
22 Store.” *Id.* at 367:19-25. Zadig also testified that advertisers had boycotted other ISPs as a result
23 of child sex abuse material on those ISPs’ services. *Id.* at 185:6-11.

24 To enforce Yahoo’s TOS, Yahoo’s moderation team proactively scans accounts for child
25 sexual abuse materials and reviews user-submitted reports of abuse. *Id.* at 186:21-187:1. After its
26 review, the moderation team may, if required by statute, file a CyberTipline Report (“CyberTip”)
27 with the National Center for Missing and Exploited Children (“NCMEC”). *Id.* at 187:1-3.

1 Yahoo’s ECIT reviews the submitted CyberTips for four criteria: (1) a child in imminent danger;
2 (2) a user in a position of authority, such as a pastor, doctor, or school teacher; (3) a user with
3 access to children; or (4) a user that is a sex offender with prior contact offenses. *Id.* at 191:14-21.
4 If any of those four criteria are met, ECIT conducts a supplemental investigation of that account,
5 related accounts, and publicly available information about the user. *Id.* at 191:22-192:1. Yahoo
6 will also deactivate an account when Yahoo files a CyberTip. *Id.* at 331:15-19.

7 **2. NCMEC CyberTips Process**

8 NCMEC, the organization to whom Yahoo sends CyberTips, is a non-governmental
9 organization in Alexandria, Virginia. Tr. at 373:17-21. By statute, any ISP like Yahoo is required
10 to send CyberTips to NCMEC to report both “apparent” or “imminent” violations of child
11 pornography statutes. 18 U.S.C. § 2258A(a). Zadig testified that not all child pornography-
12 related information is reportable to NCMEC. For example, a request for children to perform sex
13 acts over webcam is not, alone, reportable as a CyberTip. Tr. at 302:24-303:6. By contrast,
14 images or video in an account, or text conversations regarding travel for the purpose of child abuse
15 must be reported. *Id.* at 302:10-23.

16 In turn, after NCMEC reviews the CyberTip, NCMEC must make CyberTips available to
17 law enforcement, including “[a]ny Federal law enforcement agency that is involved in the
18 investigation of child sexual exploitation.” 18 U.S.C. § 2258A(c)(1). An ISP’s “knowing and
19 willful failure to make a report” is punishable by a fine of up to \$300,000. *Id.* at § 2258A(e).
20 According to FBI Special Agent Scott Schelble, NCMEC received approximately 1.5 million
21 CyberTips each month while Schelble was detailed to NCMEC between 2013 and 2015. Tr. at
22 375:3-12.

23 The FBI and other federal agencies have law enforcement agents stationed as liaisons at
24 NCMEC. *Id.* at 393:11-17. Schelble testified that at NCMEC, the FBI assists NCMEC with
25 identifying the victims in child pornography images because a victim must be identified for a
26 federal prosecution to proceed. *Id.* at 375:22-376:10. The FBI also performs a “deconfliction”
27 function to ensure that multiple federal agencies are not investigating the same target. *Id.* at

378:4-13.

3. Yahoo's First Investigation of Webcam Sexual Abuse on Yahoo's Services

In August 2014, Xoom, an online payment processing service, notified Yahoo that Xoom had identified ten Yahoo Messenger accounts in the Philippines with profile pictures of child pornography. Tr. at 193:24-194:8. Xoom told Yahoo that the ten Yahoo Messenger accounts appeared to be receiving payments "indicative of web streaming." *Id.* at 194:3-5. According to Yahoo's Sean Zadig, Yahoo conducted a limited review and confirmed that the accounts "appeared to be engaged in the sale of live stream sexual abuse of children over Yahoo Messenger – Yahoo Messenger had a webcam feature which permitted this – as well as the sale of still photographs and videos, all of which appeared to be produced from the Philippines." *Id.* at 194:22-195:2.

Yahoo also determined that the ten Yahoo Messenger accounts were interacting with other Yahoo Messenger users who were attempting to buy the material:

So the sellers, or what we call people in the Philippines offering material for sale, they were saying that they had children of certain ages who could engage in sex shows via the Yahoo Messenger webcam feature. And we observed the buyers negotiating prices or asking for specific ages of children, some extremely young, some, you know, three, four, five, or even younger, as well as requesting that specific acts be, sexual acts be taken.

Id. at 196:19-197:1. Zadig testified that Yahoo was concerned that its services were being used for realtime abuse of children:

We were extremely concerned that – and upset that there was this live streamed realtime abuse of children happening essentially right now. We – that was – that's clearly not what the product had been envisioned to do. It had been envisioned to let people communicate with friends and family and share ideas and sort of do good things, and were rather upset that this was being used in such a horrible manner.

Id. at 198:22-199:4.

In late September 2014 and early October 2014, Yahoo sent NCMEC CyberTips for the ten accounts that Xoom identified and other accounts that met NCMEC's reporting requirements. *Id.* at 199:5-14. Yahoo also sent NCMEC a supplemental report that described the relationship between the buyer and seller accounts. *See* ECF No. 119, Ex. KK. Zadig testified that Yahoo

created the supplemental report, even though NCMEC did not require it, because “there are significant brand reputational and financial impacts that could affect the company if the disclosure of this activity became, you know, became public,” such as users fleeing Yahoo services or advertisers choosing not to run ads. *Id.* at 200:1-8. Yahoo also “believed that children were being abused in realtime and we wanted to hurry and provide that quickly.” *Id.* at 200:11-13.

The supplemental report referenced the Yahoo CyberTips and stated that Yahoo determined that approximately 115 accounts were sellers. *Id.* at 407. Yahoo’s first supplemental report referred to approximately 203 “buyer” accounts that “appeared to be buying imagery, video, or live streams from the sellers.” *Id.* Yahoo then provided charts listing the seller accounts and buyer accounts. *Id.* at 408–14.

On October 3, 2014, after Yahoo submitted its first batch of CyberTips on Philippines webcam child pornography to NCMEC, Yahoo contacted NCMEC and law enforcement to set up a meeting. ECF No. 147-3 (“Schelble Decl.”), ¶ 6. Because NCMEC receives CyberTips on an individual basis, and the Yahoo reports concerned “multiple users in multiple locations engaged in realtime abuse of children,” Zadig testified that Zadig wanted to provide NCMEC and law enforcement “a full picture of what was happening” on Yahoo’s platforms. Tr. at 201:21-202:3.

On October 6, 2014, Yahoo met with NCMEC officials, FBI Special Agent Schelble, and Special Agent Neil O’Callaghan of Homeland Security Investigations (“HSI”) at NCMEC’s offices. Schelble Decl. ¶ 6. At the meeting, Zadig provided hard copies of Yahoo’s supplemental report and explained how Yahoo Messenger and its webcam feature function. Tr. at 202:10-24.

5. FBI Opens Operation Swift Traveler

After the October 6, 2014 meeting, Schelble and O’Callaghan agreed that the information in the Yahoo CyberTips and supplemental report to NCMEC warranted law enforcement investigation. Schelble Decl. ¶ 8; Tr. at 385:3-13. The FBI referred the matter to the FBI’s Major Case Coordination Unit (“MCCU”). *Id.* FBI Special Agent Jeffrey Yesensky was assigned to the MCCU from approximately August 2014 to October 2017. Tr. at 7:3-6. On November 13, 2014, Yesensky opened Operation Swift Traveler (“OST”) to investigate Philippines webcam child

pornography. ECF No. 119, Ex. X; Tr. at 14:3-7. Yesensky was MCCU's case agent on OST from November 2014 until October 2017. *Id.* at 13:20-22. Yesensky testified that during OST, he "had assistance at times from, I would say, one or at most two agents." *Id.* at 13:1-5.

MCCU is "a unit within FBI headquarters that conducts large scale international child exploitation investigations for the bureau," such as investigations involving multiple subjects or those that are resource intensive. *Id.* at 7:8-21. MCCU conducts initial investigations of potential child sexual abuse and then often refers the investigation to the relevant FBI field office. *Id.* at 8:10-20. MCCU also acts as a liaison with domestic and foreign law enforcement officials, as well as private organizations involved in preventing child sexual abuse. *Id.* at 9:10-20. Yesensky testified that discussions with private companies help the FBI understand how to seek information from those companies through legal process. *Id.* at 10:24-11:3.

As OST launched, the FBI reviewed the accounts referenced in the Yahoo CyberTips and supplemental report. *Id.* at 15:4-17. Given OST's small staff, the FBI prioritized subjects that the FBI determined to be "exigent," such as prior offenders or those in a position of trust. *Id.* at 20:23-21:4. The FBI also prioritized seller accounts and buyer accounts with conduct that was recent and actionable. *Id.* at 21:15-22:1. The MCCU then developed a "lead package," which included any content observed in the accounts, and sent the information to the FBI field office where the target was located, or to a relevant international agency. *Id.* at 22:2-8. The FBI field office would then conduct the investigation, although Yesensky and the MCCU remained available to assist. *Id.* at 32:16-25. After the first set of Yahoo CyberTips to NCMEC, the FBI obtained approximately 30 search warrants—27 for sellers and 3 for buyers. *Id.* at 79:19-80:3.

Yesensky occasionally reached out to Yahoo's Sean Zadig to clarify information around Yahoo's processes. ECF No. 119, Ex. Y. For example, in a phone call, Yesensky asked Zadig whether a Yahoo user is automatically assigned a Yahoo Messenger account. *Id.* at 1555-56.

6. Yahoo's Second Investigation of Webcam Sexual Abuse on Yahoo's Services

Yahoo continued to investigate Philippines webcam child sexual abuse on Yahoo's services. Zadig testified that Yahoo wanted to determine "if there was a rather large sort of ring or

nest of this type of activity that we were unaware of and that could be lurking and pose a significant risk for our company.” Tr. at 204:1-7. Principally, Yahoo’s second investigation sought to determine whether the buyers identified in Yahoo’s first investigation were in communication with additional sellers—which they were. *Id.* at 205:7-14. After Yahoo found those new sellers, Yahoo identified new buyers and “tried to enumerate out as best as we could all the people involved in this type of conduct.” *Id.* at 205:15-20.

After the second Yahoo investigation, Yahoo filed additional sets of CyberTips in late November 2014 and December 2014. *Id.* at 23:12-17. Yahoo prepared a second supplemental report to describe relationships between the buyer and seller accounts. *Id.* at 206:17-24. The second supplemental report listed 267 seller accounts and 347 buyer accounts, for a total of 614 accounts. ECF No. 119, Ex. DD.

On December 10, 2014, Zadig emailed Yesensky to request a meeting with the FBI and NCMEC. Ex. RR at 1693. Zadig testified that he requested the meeting “to make sure that law enforcement understood how the investigation was initiated, how it was conducted, and then we had a legal representative so they could discuss how legal process could be served.” *Id.* at 207:19-22. Yahoo also wanted to ensure that law enforcement knew that in some cases, there was “imminent travel that was going to be occurring, or individuals who had traveled previously to abuse children personally.” *Id.* at 208:25-209:4.

On December 12, 2014, Yahoo gave NCMEC its second supplemental report. Ex. RR at 2029. Zadig emailed Yesensky to inform him that Yahoo had submitted the second supplemental report, but stated that “our official data disclosure mechanism is through NCMEC so please contact them to get the data we provided.” *Id.*

On December 16, 2014, Yesensky and other federal law enforcement officials met with Zadig and Yahoo Legal Director Chris Madsen at NCMEC. ECF No. 119, Ex. DD. Zadig provided an overview of the CyberTips and second supplemental report that Yahoo had already submitted to NCMEC. *Id.* at 1561–62, 1573. The second supplemental report stated that the 347 buyer accounts “appear to be purchasing images, video, or live streams from the above seller

accounts.” ECF No. 89, Ex. E at 913.

Of note, Yahoo’s second supplemental report identified Defendant’s jrwolfen02 account as a buyer account connected to “John Wolfenbarger” in Morgan Hill, California. *Id.* at 1574. Zadig testified that Yahoo determined that Defendant’s account was in communication with two seller accounts, and that Defendant “was inquiring about, to my recollection, about the sale of child sex shows via webcam Messenger.” Tr. at 206:3-11. However, Yahoo filed no separate CyberTip for jrwolfen02, as Yahoo had not observed reportable conduct. *Id.* at 106:7-17. Zadig testified that a request for children to perform sex acts over webcam is not, alone, reportable as a CyberTip. *Id.* at 302:24-303:6.

Yesensky testified that based on the information in the second supplemental report that the FBI received from NCMEC, Defendant was not high on the FBI’s priority list. *Id.* at 158:18-159:1. Rather, the FBI again targeted seller accounts and priority buyers, or those engaged in recent and actionable conduct. *Id.* at 27:18-25. Through that process, the FBI acquired 68 more seller search warrants, which took approximately a year for the FBI to review because Yesensky had assistance from at most two other law enforcement agents from time to time. *Id.* at 28:7-17.

7. Yahoo’s Third Investigation of Child Sexual Abuse on Yahoo’s Services

In July 2015, Yahoo began a third investigation of child sexual abuse on its services. Yahoo launched the investigation after an FBI agent in Texas informed Zadig that a buyer identified in a previous Yahoo CyberTip had been arrested and “had spent approximately \$50,000 on child sex shows over the course of a few years.” Tr. at 213:20-25. Because most shows cost \$50, Zadig and Yahoo were “concerned that that amount of money might indicate that there was an even greater webcam or sex trafficking problem on Yahoo Messenger” than Yahoo had thought after its second investigation. *Id.* at 214:5-8. For the third investigation, Yahoo started by reviewing accounts that had interacted with the Texas buyer and discovered hundreds of accounts in the Philippines, many of which were “engaged in the sale of live streamed child abuse or images or video.” *Id.* at 214:10-18. Through that process, Yahoo determined that Defendant’s jrwolfen02 email account contained potential child pornography, and ECIT received authorization

from Yahoo’s legal team to review the contents of jrwolfen02 emails for the few days in which the account contained the child pornography images. *Id.* at 217:2-10.

Upon that review, ECIT determined that Defendant had committed two violations of Yahoo’s TOS: “The first was chat conversations describing an intent to purchase child abuse or, you know, web streamed child abuse; and the second was actually mail content in the user’s mailbox containing actual child pornography.” *Id.* at 220:3-6. On November 30, 2015, Yahoo submitted CyberTip 7405007 on Defendant, along with the eight images identified in Defendant’s account. ECF No. 28, Ex. D. Yahoo deactivated Defendant’s Yahoo account in December 2015. Tr. at 338:20-22.

Yahoo sent NCMEC CyberTips from its third investigation in November and December 2015. *Id.* at 224:23-25. Yahoo also sent NCMEC a third supplemental report about the connections between buyers and sellers, and Yahoo “highlighted the ones where we thought there was travel occurring, travel to the Philippines by the buyers.” *Id.* at 225:1-3.

On January 5, 2016, Zadig emailed Yesensky to request a meeting. Ex. RR at 1647. On January 21, 2016, Zadig emailed Yesensky to inform him that Yahoo had submitted its third supplemental report to NCMEC, and that Yesensky should obtain the report from NCMEC. Ex. RR at 2063. On February 3, 2016, Yesensky and other law enforcement agents met with Zadig at NCMEC. Ex. HH. Zadig testified that at the meeting, Zadig again described how Yahoo conducted its investigation and Yahoo’s more in-depth review of certain email accounts, which resulted in additional CyberTips. Tr. at 226:13-21. Because the third set of Yahoo CyberTips and third supplemental report that the FBI received from NCMEC identified approximately 250 buyer accounts and approximately 50 seller accounts, Yesensky testified the FBI again prioritized investigation of accounts engaged in recent and actionable conduct. *Id.* at 31:7-16.

8. The FBI Prioritizes Defendant

Yesensky testified that the FBI first became specifically aware of Defendant in February 2016 based on CyberTip 7405007. Tr. at 39:15-20; 44:15-19. The CyberTip stated that the incident type was “Child Pornography (possession, manufacture, and distribution)” and that

1 Yahoo had observed and reviewed eight images of child pornography in an email dated December
2 2, 2013. ECF No. 28, Ex. D at 1073–75.

3 On March 11, 2016, Yesensky sent a lead package on Defendant to the FBI’s San
4 Francisco field office. ECF No. 85, Ex. D. The lead package included CyberTip 7405007, the
5 images included in the CyberTip, and records checks that MCCU conducted to determine that
6 Defendant was the likely user of jrwolfen02. *Id.* at 1095; *id.* at 39:24-40:7. Later, Yesensky
7 scanned the results of search warrants on OST seller accounts for the term “jrwolfen02” and
8 discovered Yahoo Messenger chats between jrwolfen02 and approximately 11 webcam child
9 pornography seller accounts in the Philippines. *Id.* at 40:10-15. Yesensky forwarded that
10 additional information to the FBI’s San Francisco field office on July 13, 2016. Ex. D at 1097.

11 In 2016, FBI Special Agent Chris Marceau was assigned to the San Francisco field office
12 and specifically to a San Jose unit that investigated violent crimes against children. Tr. at 402:3-8.
13 Marceau testified that based on the lead package, the FBI served a search warrant for jrwolfen02
14 on Yahoo on May 9, 2016. *Id.* at 404:23-25; *see* ECF No. 28, Ex. A (search warrant). The search
15 warrant application was signed by FBI Special Agent Ann Trombetta, who also submitted an
16 affidavit with the warrant application. *Id.* at 11.

17 In that affidavit, Trombetta explained that Yahoo’s ECIT had conducted an investigation
18 of Philippines webcam sexual abuse on Yahoo’s services and had submitted CyberTips and
19 supplemental reports to NCMEC. *Id.* ¶¶ 35–36. Trombetta attested that the FBI had obtained
20 search warrants for several seller accounts beginning in February 2015. *Id.* ¶ 39. As to
21 Defendant, Trombetta described the eight images in Defendant’s account, which “all appeared to
22 be photographs of two girls who appear to be under twelve years old, performing sexual acts on
23 themselves.” *Id.* ¶ 38. Trombetta attested that Yahoo had reported the images in Defendant’s
24 account in a CyberTip on November 30, 2015. *Id.* ¶ 40. United States Magistrate Judge
25 Nathanael Cousins issued the search warrant. *Id.* at 11.

26 Special Agent Marceau testified that the search warrant on Defendant’s Yahoo account
27 returned “child exploitation images, videos, and still pictures, as well as numerous chats

identifying the rape of children, the exploitation of minors, and numerous instances requesting more of the same.” Tr. at 405:14-17.

After the FBI executed the search warrant, Marceau spoke with Defendant twice. First, Marceau spoke to Defendant on August 2, 2016 after Defendant arrived at San Francisco International Airport (“SFO”). *Id.* at 405:23-406:1. Second, Marceau spoke with Defendant on August 31, 2016 in the parking lot of a coffee shop in Morgan Hill, California. *Id.* at 406:6-17. Marceau testified that Defendant arrived voluntarily and “was helping us identify his victims so that we can recover those victims from being exploited by other subjects.” *Id.* at 407:17-19. Defendant executed an FD 1086 form with his consent for the FBI to assume Defendant’s online identity and to search Defendant’s Yahoo and AOL accounts. *Id.* at 407:21-410:21. However, none of Defendant’s passwords worked, and the FBI was unable to assume Defendant’s online identity. Tr. at 410:5-7.

On December 15, 2016, Defendant was indicted. ECF No. 1.

As of early 2019, OST remains ongoing, although Special Agent Kelly Clark has taken over for Yesensky. Tr. at 14:19-22. Yesensky estimated that during his time leading OST, MCCU sent “close to 200” lead packages to domestic FBI field offices and to international FBI partners. *Id.* at 33:4-11.

As for Yahoo, ECIT conducted a fourth investigation of Philippines webcam child pornography on Yahoo services in 2018 after Xoom notified Yahoo of additional accounts that appeared to be engaged in webcam child sexual abuse. *Id.* at 227:2-9. ECIT sent CyberTips related to that investigation to NCMEC in April 2019. *Id.*

B. Procedural History

On December 15, 2016, a federal grand jury indicted Defendant on one count of attempted production of child pornography, in violation of 18 U.S.C. § 2251(c) and (e); one count of attempted coercion and enticement of minors, in violation of 18 U.S.C. § 2422(b); and one count of receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2). ECF No. 1.

On December 6, 2017, Defendant filed his first motion to compel production of evidence

1 under Federal Rule of Criminal Procedure 16 and *Brady*. ECF No. 28. Defendant requested all
2 documents related to cases filed in this district from 2010 to 2016 in which the government relied
3 on Yahoo’s search of an email account. *Id.* at 4; ECF No. 189 at 1 n.1. Defendant contended that
4 the documents were relevant to a future motion to suppress evidence under *Walther*. ECF No. 28
5 at 8–10.

6 On December 21, 2017, the Court referred Defendant’s first motion to compel to
7 Magistrate Judge Nathanael Cousins. ECF No. 30. On January 12, 2018, Judge Cousins denied
8 without prejudice Defendant’s first motion to compel because Defendant had not established that
9 the files from all OST investigations other than that of Defendant were material, and because
10 Defendant’s “request for review of prosecution files from 2010 to 2016 is a speculative fishing
11 expedition.” ECF No. 43 at 5.

12 On February 28, 2018, Defendant moved to suppress Defendant’s August 2016 statements
13 to Special Agent Marceau. ECF No. 49. In the afternoon of April 17, 2018, after the motion was
14 fully briefed and less than 24 hours before the April 18, 2018 evidentiary hearing on Defendant’s
15 first motion to suppress, Defendant withdrew the motion. ECF No. 73.

16 On May 25, 2018, Defendant filed his second motion to compel and requested production
17 of “[a]ll reports and documents generated between 2013 and 2018 by the FBI, the Department of
18 Homeland Security, the Department of Justice, and/or any other involved agency, pertaining to the
19 Philippines webcam investigation involving Xoom and Yahoo!.” ECF No. 85 at 7.

20 On July 2, 2018, Judge Cousins granted Defendant’s motion to compel. ECF No. 109.
21 Judge Cousins held that “the government must search all Operation Swift Traveler Files,
22 investigations, notes, communications, and prosecutions for responsive information.” *Id.* at 5.

23 On July 16, 2018, pursuant to Federal Rule of Criminal Procedure 59(a), the government
24 filed an objection to Judge Cousins’ July 2, 2018 order requiring the government to produce
25 materials from all OST investigations. ECF No. 111. The government contended that
26 Defendant’s request was a “pure fishing expedition” and that the order was unduly burdensome
27 because to comply with the order, “the government would have to locate and produce, wholesale,

1 hundreds of investigative lead files, internal case files, prosecution files, grand jury investigation
2 files, and all legal process sought and obtained” from those other investigations. *Id.* at 4–6.

3 Nonetheless, the government produced other materials to Defendant, including
4 “communications between the FBI’s Major Case Coordination Unit (MCCU) and Yahoo
5 representatives.” ECF No. 117, Ex. G.

6 On September 5, 2018, the Court held a hearing on the government’s objection to Judge
7 Cousins’ July 2, 2018 order. ECF No. 126.

8 On October 10, 2018, the Court sustained the government’s objection to Judge Cousins’
9 July 2, 2018 order. ECF No. 132. The Court discussed the standard applicable to the instant
10 motion to suppress and noted that “some discovery related to a pattern of activity is needed” for
11 Defendant to contend that Yahoo, Xoom, and/or NCMEC acted as government agents. *Id.* at 2, 7.
12 However, the Court held that Defendant’s request for discovery of *all* OST investigations
13 involving targets other than Defendant was overbroad because to respond, the government would
14 have to “contact the field offices and Legal Attaches that received the 195 leads to determine
15 whether a case was opened, request the case files and all comments and notes, and search for
16 email and other communications outside the case files after identifying all relevant custodians.”
17 *Id.* at 9. Such discovery was “akin to the speculative fishing expedition that Defendant sought in
18 his first motion to compel and that the Magistrate Judge rejected” as immaterial. *Id.* at 10.
19 Accordingly, the Court sustained the government’s objection and remanded to Judge Cousins “for
20 further proceedings to determine the proper scope of discovery.” *Id.*

21 On November 30, 2018, Defendant filed his third motion to compel, in which Defendant
22 stated that the government had produced “additional documents held by MCCU regarding Mr.
23 Zadig, Yahoo, and OST” and relevant emails between Yahoo and “the thirteen most active agents
24 within MCCU in relation to OST.” ECF No. 143 at 2. However, Defendant requested e-mail
25 communications between “field agents handling the OST cases and Yahoo!, Xoom and NCMEC.”
26 *Id.*

27 On April 8, 2019, Judge Cousins denied Defendant’s third motion to compel. ECF No.

175. Judge Cousins held that the government’s production of relevant emails between the thirteen most active MCCU agents and Yahoo satisfied the government’s obligation to “use ‘affirmative due diligence’ to gather exculpatory material from known and plausible sources.” *Id.* at 3–4 (citing *United States v. Cerna*, 633 F. Supp. 2d 1053, 1061 (N.D. Cal. 2009)).

On April 22, 2019, Defendant filed an objection to Judge Cousins’ April 8, 2019 order denying Defendant’s third motion to compel. ECF No. 180. On May 7, 2019, pursuant to Civil Local Rule 72-2, this Court deemed denied Defendant’s objection. ECF No. 181.

On June 12, 2019, Defendant filed the instant motions to suppress, including a motion to suppress evidence pursuant to *Walther*, ECF No. 183 (“Mot.”), and a motion to suppress evidence pursuant to *Franks*. ECF No. 184. Defendant also filed a fourth motion to compel production. ECF No. 186.

On June 26, 2019, the government filed oppositions to Defendant’s motions to suppress, ECF No. 188 (“Opp.”) & 190, and an opposition to Defendant’s fourth motion to compel. ECF No. 189. On July 3, 2019, NCMEC filed an amicus brief in support of the government’s opposition to Defendant’s fourth motion to compel. ECF No. 192. On July 3, 2019, Defendant filed replies in support of his motions to suppress, ECF Nos. 194 (“Reply”) & 195, and in support of his fourth motion to compel. ECF No. 193.

On July 11, 2019, the Court denied Defendant’s fourth motion to compel. ECF No. 198. The Court explained that Defendant broadly requested all communications that pertain to the Philippines webcam investigations/Operation Swift Traveler. *Id.* at 13. The Court held that Defendant’s request was overbroad, would impose a substantial burden on the government, and that Defendant had failed to show that such communications were material to Defendant’s motion to suppress—particularly in light of the extensive communications between the FBI’s MCCU and Yahoo that the government had already produced to Defendant. *Id.* at 14, 19–20.

On July 12, 2019 and July 23, 2019, the Court held an evidentiary hearing on Defendant’s motion to suppress pursuant to *Walther*. ECF Nos. 199, 203. FBI Special Agent Jeff Yesensky, Yahoo’s Sean Zadig, FBI Special Agent Scott Schelble, and FBI Supervisory Special Agent Chris

Marceau testified at the hearing.

II. LEGAL STANDARD

The Fourth Amendment of the U.S. Constitution provides that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. As a general matter, the exclusionary rule applies to “primary evidence obtained as a direct result of an illegal search” as well as “evidence later discovered and found to be derivative of an illegality.” *Utah v. Strieff*, 136 S. Ct. 2056, 2061 (2016) (quoting *Segura v. United States*, 468 U.S. 796, 804 (1984)). However, because exclusion of evidence hinders the truth-seeking process, courts generally must weigh whether the “deterrence benefits” of applying the exclusionary rule “outweigh [the] substantial social costs.” *Hudson v. Michigan*, 547 U.S. 586, 591 (2006) (internal quotation marks and citation omitted).

“The proponent of a motion to suppress has the burden of establishing that his own Fourth Amendment rights were violated by the challenged search or seizure.” *Rakas v. Illinois*, 439 U.S. 128, 130 n.1 (1978); *see also United States v. Willis*, 431 F.3d 709, 715 n.5 (9th Cir. 2005) (“The defendant has the burden of proof on a motion to suppress evidence.”); *United States v. Caymen*, 403 F.3d 1196, 1199–2000 (9th Cir. 2005). “Initially, the defendant who shows that he was the victim of an unconstitutional search must go forward with specific evidence demonstrating taint.” *United States v. Cella*, 568 F.2d 1266, 1284–85 (9th Cir. 1977); *United States v. Kandik*, 633 F.2d 1334, 1335 (9th Cir. 1980) (“[A] defendant has the initial burden of establishing a factual nexus between the illegality and the challenged evidence.”).

Once the defendant satisfies his burden, “[t]he burden then shifts to the government to show that it acquired its evidence from an independent source,” *Cella*, 568 F.2d at 1285, or that another exception, such as the good faith exception, applies, *United States v. Michaelian*, 803 F.2d 1042, 1048 (9th Cir. 1986) (“The government, not the defendant, bears the burden of proving that its agents’ reliance upon the warrant was objectively reasonable.”); *see also United States v.*

Camou, 773 F.3d 932, 944 (9th Cir. 2014) (“When the officer executing an unconstitutional search acted in ‘good faith,’ or on ‘objectively reasonable reliance,’ the exclusionary rule does not apply. . . . The burden of demonstrating good faith rests with the government.”). The standard of proof for either party “should impose no greater burden than proof by a preponderance of the evidence.” *Nix v. Williams*, 467 U.S. 431, 444 & n.5 (1984).

III. DISCUSSION

Before the Court are two motions to suppress. Both arise from Defendant’s core contention that Yahoo’s search of Defendant’s Yahoo email account violated the Fourth Amendment. In Defendant’s motion to suppress pursuant to *Walther*, Defendant contends that the Fourth Amendment requires suppression of the fruits of Yahoo’s search. In Defendant’s *Franks* motion to suppress, Defendant contends that the magistrate judge would not have issued the search warrant for Defendant’s Yahoo account had the FBI’s affidavit described Yahoo’s search in detail. Defendant argues that the details of Yahoo’s search would have alerted the magistrate judge to the illegality of Yahoo’s search. Accordingly, if Yahoo’s search was not illegal, Defendant’s *Franks* motion also fails. The Court first discusses Defendant’s motion to suppress pursuant to *Walther* and then discusses Defendant’s *Franks* motion.

A. Defendant’s Motion to Suppress Under *Walther*

In his motion to suppress under *Walther*, Defendant contends that Yahoo’s search of the eight child pornography images in Defendant’s Yahoo email account violates the Fourth Amendment because Yahoo acted as a government agent when Yahoo conducted the search. The government raises three arguments in response: (1) Defendant lacked a reasonable expectation of privacy in his Yahoo account because Defendant consented to the search via Yahoo’s terms of service (“TOS”); (2) Yahoo did not act as a government agent; and (3) even if Yahoo’s search violated the Fourth Amendment, the Court should apply the good faith exception to the exclusionary rule. Opp. at 6, 10, 24.

As set forth below, the Court agrees with the government that Yahoo did not act as a government agent and that, even if it had, the good faith exception to the exclusionary rule applies

here. These findings are fatal to Defendant’s motion to suppress under *Walther*. Consequently, the Court need not reach the government’s first argument—that Defendant lacked a reasonable expectation of privacy in his Yahoo account.

1. Yahoo’s Access of Defendant’s Email Account was not Government Action

The Court begins with Defendant’s contention that Yahoo’s search was government action. The United States Supreme Court has consistently construed the Fourth Amendment’s protections “as proscribing only governmental action.” *United States v. Al Nasser*, 555 F.3d 722, 725 (9th Cir. 2009) (quoting *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)). Accordingly, a wrongful search or seizure by a private party does not violate the Fourth Amendment unless the private party acts as an “instrument or agent” of the state in effecting a search or seizure. *Walther*, 652 F.2d at 791; *see also Skinner v. Railway Labor Executives’ Ass’n*, 489 U.S. 602, 614 (1989) (explaining that the Fourth Amendment “does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative”).

In the Ninth Circuit, “[t]he general principles for determining whether a private individual is acting as a governmental instrument or agent for Fourth Amendment purposes have been synthesized into a two part test.” *United States v. Reed*, 15 F.3d 928, 931 (9th Cir. 1994). Under that test, the Court inquires “(1) whether the government knew of and acquiesced in the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or further his own ends.” *Id.* The Ninth Circuit has also explained that a private party’s “legitimate, independent motivation” to further its own ends is “not negated by any dual motive to detect or prevent crime or assist the police.” *United States v. Cleaveland*, 38 F.3d 1092, 1094 (9th Cir. 1994), *as amended* (Jan. 12, 1995).

For example, in *United States v. Young*, the Ninth Circuit rejected a defendant’s contention that the government knew of and acquiesced in FedEx’s search of the defendant’s package where “the FedEx security officer opened the package on his own initiative pursuant to FedEx security policies.” 153 F.3d 1079, 1080 (9th Cir. 1998). The FedEx security officer suspected that the package contained methamphetamine and contacted the DEA, which then obtained a warrant and

1 arrested the defendant. *Id.* The Ninth Circuit observed that FedEx had developed its security
2 policies not to assist law enforcement, but rather to protect employee safety and to avoid tempting
3 FedEx employees to steal packages. *Id.* at 1081. FedEx couriers had been killed after packages
4 delivering drugs were not delivered, and flammable drugs posed a serious safety hazard to FedEx
5 employees and the public. *Id.* Accordingly, the defendant failed to show that FedEx acted as an
6 instrument or agent of the government. *Id.*

7 **a. Yahoo Initiated its Third Investigation of its Own Accord**

8 In the instant case, Defendant has failed to show that Yahoo acted as an instrument or
9 agent of the government. When Yahoo searched Defendant’s email account in 2015, Yahoo acted
10 on its own initiative. In July 2015, Yahoo began its third investigation into Philippines webcam
11 pornography on Yahoo’s services after Yahoo learned that a Yahoo Messenger user in Texas had
12 spent \$50,000 on child sex shows. Tr. at 213:20-25. Because most shows cost \$50, Yahoo was
13 “concerned that that amount of money might indicate that there was an even greater webcam or
14 sex trafficking problem on Yahoo Messenger” than Yahoo had thought after its second
15 investigation, which had concluded in late 2014. *Id.* at 214:5-8. Yahoo’s Sean Zadig explicitly
16 testified that law enforcement did not ask Yahoo to initiate its third investigation. *Id.* at 214:22-
17 24. Rather, Zadig testified that Yahoo monitors its services for child pornography to create a “safe
18 place” for its users—many of whom are minors themselves—and to protect Yahoo’s
19 advertisement revenue stream. *Id.* at 182:20-183:4. A person as young as 13 years old can create
20 a Yahoo account. *Id.* at 186:6-8.

21 In testimony, Zadig provided numerous examples of how child pornography on Yahoo’s
22 services could threaten Yahoo’s advertisement revenue. After Google detected child pornography
23 on several blogs on Tumblr—which Yahoo owns—Google threatened to suspend Tumblr from
24 Google’s AdSense network. *Id.* at 184:9-14. In December 2018, Apple also temporarily blocked
25 Tumblr’s app from the Apple App Store “because Apple had detected child pornography on one
26 single blog within the Tumblr ecosystem.” *Id.* at 184:15-20. Both actions posed a significant
27 revenue threat to Yahoo. Without a presence in the App Store, for example, no new mobile user

could access Tumblr and view ads on Tumblr. *Id.* at 185:21-25. Yahoo’s investigations of violations of its TOS and attempts to remove child pornography are factors that “allowed Apple to let us relist the Tumblr app on the App Store.” *Id.* at 367:19-25. Zadig also testified that advertisers had boycotted other ISPs as a result of child sex abuse material on those ISPs’ services. *Id.* at 185:6-11. Thus, Yahoo had its own “legitimate, independent motivation” for conducting its third investigation to remove child pornography from its services. *See Cleaveland*, 38 F.3d at 1094 (holding that a private citizen’s “legitimate, independent motivation” for a search is “not negated by any dual motive to detect or prevent crime or assist the police”).

In that third investigation, Yahoo reviewed accounts that had interacted with the Texas user, discovered numerous new webcam seller accounts in the Philippines, and then reviewed accounts of buyers that interacted with those seller accounts. *Id.* at 215:19-23. Through that process, Yahoo determined that Defendant’s jrwolfen02 Yahoo email account contained child pornography images and that Defendant had engaged in “chat conversations describing an intent to purchase child abuse or, you know, web streamed child abuse.” *Id.* at 220:3-6. Then, pursuant to Yahoo’s NCMEC reporting requirements, Yahoo submitted CyberTip 7405007 on Defendant on November 30, 2015. ECF No. 28, Ex. D.

In February 2016, NCMEC sent the FBI’s MCCU CyberTip 7405007, as NCMEC is required by statute to send CyberTips to the relevant law enforcement agency after NCMEC reviews the CyberTip “in furtherance of its nonprofit mission.” *Tr.* at 44:15-19; *see* 18 U.S.C. § 2258A(c). Then, the MCCU investigated Defendant and referred the case to the FBI’s San Francisco field office for further investigation. ECF No. 85, Ex. D. Defendant identifies no evidence that the FBI encouraged or acquiesced in Yahoo’s third investigation.

Moreover, district and circuit courts around the country—including in this district—have universally rejected arguments like Defendant’s. The Court now discusses those cases.

b. Courts Have Rejected the Contention that Yahoo and Zadig Acted as Government Agents

In fact, one district court has already denied a motion to suppress based on the same Yahoo

investigations into Philippines webcam child pornography as in the instant case, *United States v. Rosenow*, 2018 WL 6064949 (S.D. Cal. Nov. 20, 2018), and another district court has denied a motion to suppress contending that Zadig, when employed at Google, acted as a government agent. *United States v. Drivdahl*, 2014 WL 896734 (D. Mont. Mar. 6, 2014).

In *Rosenow*, Yahoo identified Rosenow as a buyer in Yahoo’s second supplemental report sent to NCMEC on December 5, 2014. 2018 WL 6064949, at *2. Based on Yahoo’s reports to NCMEC, the FBI identified Rosenow as a suspect and referred the investigation to law enforcement agents in San Diego in February 2015. *Id.* at *3. Then, in Yahoo’s third investigation, Yahoo found chats in which Rosenow “described upcoming travel plans to the Philippines and the abuse of children.” *Id.* at *4. As a result, Yahoo filed a CyberTip on Rosenow on December 2, 2015. *Id.* NCMEC processed the CyberTip and forwarded it to the FBI on December 23, 2015. *Id.* In January 2017, an FBI agent in San Diego began investigating whether Rosenow was involved in child sexual abuse. *Id.* In June 2017, the FBI executed search warrants on Rosenow’s person, digital devices, and home. *Id.* at *5–6.

Rosenow moved to suppress all evidence because, he contended, the government violated the Fourth Amendment “by repeatedly accepting private communications from Yahoo.” *Id.* at *6. The district court denied Rosenow’s motion to suppress. The district court observed that Rosenow failed to adduce any evidence that law enforcement encouraged any of Yahoo’s Philippines webcam investigations. *Id.* at *7. Further, the FBI only sought and received assistance from Yahoo personnel through “legal process.” *Id.* at *8. The district court also explained that Yahoo had an independent business interest in “ensuring that its products are free of illegal conduct, in particular, child sexual abuse material,” and that Yahoo had conducted its investigations for those purposes. *Id.* Thus, the district court concluded that Yahoo was acting “in a private capacity not subject to Fourth Amendment constraints” when Yahoo initiated the investigation. *Id.* Moreover, Yahoo’s compliance with its statutory duty to report known child pornography to NCMEC “did not convert Yahoo ECIT into a government actor.” *Id.* at *9. Most importantly, the NCMEC statute “imposed no duty on Yahoo to *monitor* its platform for child exploitation materials.” *Id.* at

*10 (emphasis added).

Similarly, the district court in *Drivdahl* denied a motion to suppress in which Drivdahl argued that Sean Zadig, in his former capacity as an investigator at Google, had acted as a government agent. 2014 WL 896734. In *Drivdahl*, as in the instant case, Zadig had submitted CyberTips and then prepared a supplemental report for NCMEC to explain the connections between various Google accounts engaged in the transmission and solicitation of child pornography images. *Id.* at *3.

Drivdahl contended that Zadig and the FBI had “teamed up” for Zadig to construct the supplemental report. *Id.* However, as with Yahoo’s supplemental reports in the Philippines webcam investigation, Zadig did not speak to any law enforcement officer about the subject matter of the report until after Zadig submitted the supplemental report to NCMEC. *Id.* Accordingly, the district court determined that there was “simply no evidence” that any government agent was even aware of Zadig’s investigation, “let alone acquiesced or encouraged it.” *Id.* Zadig’s conversations with law enforcement after Zadig submitted the CyberTips and supplemental report “were limited to general questions about Google services and to Zadig explaining the information that had been reported in the CyberTips and his supplement.” *Id.* at *4. Likewise, in the instant case, Defendant identifies no evidence that Zadig or anyone from Yahoo ever provided the FBI with information outside of Yahoo’s submissions to NCMEC and the service of legal process.

c. District Courts in this District and Circuit Courts Around the Country Have Rejected Defendant’s Arguments

Furthermore, district courts in this district and circuit courts around the country have repeatedly rejected the contention that an ISP’s search of its own user’s account and subsequent report to NCMEC of child pornography renders the ISP a government agent.

For example, in *Viramontes*, Dropbox used an automated search tool to discover ten apparent child pornography videos in Viramontes’s Dropbox account. *United States v. Viramontes*, 16-CR-508-EMC, ECF No. 62 (N.D Cal. Nov. 14, 2017), slip op. at 2. Dropbox opened the files to confirm that the videos were child pornography and then sent NCMEC a

CyberTip with the ten videos attached. *Id.* at 3. NCMEC confirmed that the videos contained child pornography, determined that Viramontes was located in the Bay Area, and forwarded the CyberTip to the San Jose Police Department. *Id.* Viramontes moved to suppress the evidence on the basis that Dropbox acted as a government agent when Dropbox searched Viramontes’s Dropbox account. *Id.*

The district court rejected Viramontes’s argument. The district court explained that there was no evidence that the government was aware of or acquiesced to Dropbox’s automated or manual searches of Viramontes’s account in particular. *Id.* at 4–6. The district court also explained that Dropbox had a “legitimate, independent motivation” to search user accounts. *Id.* at 8. Specifically, and similarly to Yahoo in the instant case, Dropbox wished to avoid becoming a repository for child pornography because “users may stop using our services if they encounter it.” *Id.* Dropbox also conducted manual review of user accounts after its automated searches to ensure that Dropbox submits CyberTips to NCMEC only for reportable content. *Id.* at 10. Accordingly, the district court held that Dropbox did not act as a government agent when searching its users’ accounts and reporting child pornography to NCMEC.

Likewise, the district court in *United States v. Lien* denied a motion to suppress alleging that Google acted as a government agent when Google searched Lien’s Google account. 2017 U.S. Dist. LEXIS 188903 (N.D. Cal. May 10, 2017). In *Lien*, Google used a “hash” technology to identify three suspected child pornography images in Lien’s Google Photos account. *Id.* at *1–2. A Google employee opened the images and confirmed that they depicted child pornography. *Id.* at *2. Three days later, Google submitted a CyberTip to NCMEC with the three images. *Id.* NCMEC was able to link the user account information to Lien “and discover that Lien has a 2012 felony conviction for distribution of child pornography.” *Id.* NCMEC forwarded the CyberTip to the San Francisco Police Department, which obtained and executed a warrant on Lien’s Google account. *Id.* at *2–3.

The district court denied Lien’s motion to suppress. The district court explained that Google monitors its services for illegal content because “users will stop using [the] services if they

1 become associated with being a haven for abusive content.” *Id.* at *7 (alteration in original).
2 Google also conducts both automated and manual reviews of images for quality control purposes.
3 *Id.* at *9. Thus, Google did not act at the government’s direction, and Lien failed to show that
4 Google “was principally motivated to assist law enforcement” when Google searched Lien’s
5 Google Photos account. *Id.* at *10–11.

6 Circuit courts have reached similar conclusions about ISP searches of user accounts that
7 lead to NCMEC CyberTips. For example, in *United States v. Cameron*, 699 F.3d 621 (1st Cir.
8 2012), Yahoo discovered child pornography images in Cameron’s Yahoo Photo account after
9 receiving an anonymous tip. *Id.* at 628. Yahoo then sent NCMEC a CyberTip. *Id.* at 629.
10 NCMEC later forwarded the CyberTip to law enforcement officers in Maine, who determined that
11 Cameron was associated with the Yahoo Photo account. *Id.* The police obtained and executed
12 search warrants on Cameron’s home and Yahoo accounts, and discovered child pornography
13 images at Cameron’s home and in his Yahoo accounts. *Id.* at 630.

14 To determine whether a private search qualifies as government action, the First Circuit
15 examines (1) the extent of the government’s role in “instigating or participating in the search”; (2)
16 the government’s intent and degree of control over the private party; and (3) whether the private
17 party aims to help the government or further its own interests. *Id.* at 637. Thus, the First Circuit’s
18 test resembles the Ninth Circuit’s test, which also focuses on government acquiescence and the
19 private party’s purpose in conducting the search.

20 The First Circuit applied its three-factor test and concluded that all three demonstrated that
21 Yahoo’s search was not government action. First, Yahoo, not the government, instigated the
22 search after Yahoo received an anonymous tip. *Id.* Second, there was no evidence that the
23 government controlled Yahoo’s search. *Id.* Moreover, Yahoo’s NCMEC reporting requirement
24 imposed no duty on Yahoo to *search* for child pornography, but only to *report* child pornography
25 of which it became aware. *Id.* at 638. Third, although combating child pornography is a
26 government interest, the First Circuit held that “this does not mean that Yahoo! cannot voluntarily
27 choose to have the same interest” and do so for its own business purposes. *Id.*

The Fourth and Eighth Circuits have also held that compliance with NCMEC reporting requirements does not transform an ISP into a government agent. *United States v. Richardson*, 607 F.3d 357, 367 (4th Cir. 2010) (“We conclude that the statutory provision pursuant to which AOL reported Richardson’s activities did not effectively convert AOL into an agent of the Government for Fourth Amendment purposes.”); *see also United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013) (“A reporting requirement, standing alone, does not transform an Internet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography.”).

d. Defendant’s Cases Also Hold that ISPs are Not Government Agents

Moreover, the Tenth Circuit—in a case Defendant cites—has also concluded that an ISP does not act as a government agent when the ISP searches a user’s account for child pornography. *See* Mot. at 4. In *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016) (Gorsuch, J.), AOL conducted a hash search of Ackerman’s AOL email account. AOL logged hash values for images that AOL employees had previously reviewed and determined were child pornography. *Id.* at 1294. Then, via an automated search tool, AOL compared the hash values of images in AOL accounts to the hash values of the known child pornography images. *Id.* Based on a hash search, AOL determined that four images in Ackerman’s account were child pornography, but AOL did not open and review the images before AOL sent a CyberTip to NCMEC. *Id.* A NCMEC analyst then opened and reviewed the images to confirm that they were child pornography images. *Id.*

The Tenth Circuit assumed that AOL’s search was a private search not subject to Fourth Amendment protections, and addressed only whether NCMEC’s search violated the Fourth Amendment. *Id.* at 1295. Thus, the Tenth Circuit, like all of the other circuit courts and district courts to address Defendant’s arguments, also concluded that an ISP’s search of its user’s accounts does not violate the Fourth Amendment.

In the remainder of *Ackerman*, the Tenth Circuit concluded that NCMEC—which opened and reviewed the images, whereas AOL did not—acted as a government agent due to NCMEC’s “special law enforcement duties and powers.” *Id.* at 1296. That aspect of *Ackerman* is not

relevant to the instant case, in which Defendant attacks *Yahoo's* search, not NCMEC's search. Nor does Defendant in the instant case contend that NCMEC and not Yahoo manually opened and reviewed the images in Defendant's Yahoo account. Indeed, CyberTip 7405007 shows that Yahoo opened and reviewed the eight images in Defendant's Yahoo account before Yahoo sent the CyberTip to NCMEC. ECF No. 28, Ex. D.

In the other ISP search case that Defendant cites, *United States v. Keith*, 980 F. Supp. 2d 33 (D. Mass. 2013), the court again concluded that an ISP's search of its user's account was not government action. In *Keith*, AOL filtered its network for suspected child pornography "[t]o prevent its communications network from serving as a conduit for illegal activity." *Id.* at 36. AOL used its hash search tool to determine that Keith's AOL account contained image files that matched child pornography images, but AOL did not open and review the images before AOL sent a CyberTip to NCMEC. *Id.* at 37. NCMEC then opened and viewed the images and confirmed that the images contained child pornography. *Id.* at 37–38. The district court expressly held that AOL was not a government agent for Fourth Amendment purposes because AOL's hash search was "motivated by its own wholly private interests in seeking to detect and deter the transmission of child pornography through its network facilities." *Id.* at 40. The district court also observed that "[t]he government exercises no control over AOL's monitoring of its network." *Id.* Thus, *Keith* too supports the conclusion that Yahoo's search in the instant case was not government action.

The district court in *Keith* went on to hold that when NCMEC viewed the images, NCMEC acted as a government agent because NCMEC's search was "conducted for the sole purpose of assisting the prosecution of child pornography crimes." *Id.* at 41. *Keith's* conclusion about NCMEC's search is not relevant to the instant case, in which Defendant contends only that Yahoo's search—not NCMEC's—was government action. Regardless, in *Keith*, the district court applied the good faith exception to the exclusionary rule and denied suppression because NCMEC had no notice that its actions were unconstitutional. *Id.* at 46. As a result of *Keith*, NCMEC CyberTip forms now include a box where an ISP may indicate whether the ISP opened and

reviewed the images in the CyberTip. Tr. at 389:6-8.

Accordingly, even in the ISP search cases that Defendant cites, the Tenth Circuit and District of Massachusetts concluded that an ISP's search of its own user's account for child pornography was not government action. In fact, Defendant cites no ISP search case in which a court has concluded that an ISP's search for child pornography constituted government action.

e. Walther is Distinguishable

Instead, Defendant depends on *United States v. Walther*, a Ninth Circuit case from the 1980s that did not involve an ISP's search of its user's account. However, *Walther* is readily distinguishable. In *Walther*, an airline employee acted as a paid DEA informant. 652 F.2d at 790. Over four years, the DEA paid the employee for at least eleven reports of "suspicious individuals fitting the 'drug profile'" at the ticket counter. *Id.* The employee had also opened approximately ten packages called SpeedPaks to search for illegal drugs. *Id.* According to a DEA agent, the DEA would have paid the employee "had he ever discovered a significant amount of drugs" in a SpeedPak. *Id.* After the employee opened one SpeedPak and discovered a white powder, the employee reported the discovery to the DEA, which later arrested Walther. *Id.* The district court found that the airline employee acted as an "instrument or agent" of the DEA and suppressed the evidence. *Id.* at 791. When searching the SpeedPak, the employee "was not carrying out a business purpose of his employer, his sole reason being his suspicion that the case contained illegal drugs" and the employee "probably opened the case with the expectation that he would be compensated by the DEA if he were to discover a significant quantity of illegal drugs." *Id.*

The Ninth Circuit upheld the suppression because the airline employee did not open the SpeedPak out of "legitimate business considerations," but rather *only* because he suspected that the SpeedPak contained illegal drugs and that the DEA might pay him for the discovery. *Id.* at 792. In addition, the DEA had encouraged the airline employee to engage in the search because the DEA had previously paid the employee for drug-related information and had never discouraged him from opening SpeedPaks. *Id.* at 793. Thus, the DEA's encouragement and payments proved the government's acquiescence in the employee's search. *Id.* However, the

Ninth Circuit emphasized the “narrowness of our holding,” and stated that its opinion did not “diminish the duty of any private citizen to report possible criminal activity.” *Id.*

Courts considering motions to suppress based on ISP reports to NCMEC have consistently “distinguished *Walther*.” *Lien*, U.S. Dist. LEXIS 188903, at *7 (citing *United States v. Green*, 857 F. Supp. 2d 1015, 1018 (S.D. Cal. 2012)). They have done so on the ground that ISPs, unlike the employee in *Walther*, are not paid informants and are not motivated by the promise or potential of a government reward. *Id.*; see also *United States v. Snowadzki*, 723 F.2d 1427, 1430 (9th Cir. 1984) (distinguishing *Walther* because “there is no evidence that the seizure was motivated by IRS prompting or encouragement”).

The instant case is no different. Defendant identifies no evidence that the FBI paid or rewarded Yahoo for any of Yahoo’s CyberTips, or that Yahoo conducted its investigations of child sexual abuse on Yahoo’s services because Yahoo expected a reward from the government.

Rather, unlike the employee in *Walther*, Yahoo prohibits child pornography material on its services and enforces that prohibition for its own independent business reasons. Specifically, Yahoo worries that users may leave Yahoo’s services if they view Yahoo’s services as unsafe, as a person as young as 13 years old can create a Yahoo account. Tr. at 186:6-8. In addition, Yahoo is concerned that advertisers may decline to advertise on Yahoo if Yahoo services are havens for child pornography. *Id.* at 200:1-8.

For example, Zadig testified that after Google detected child pornography on several blogs on Tumblr—which Yahoo owns—Google threatened to suspend Tumblr from Google’s AdSense network. *Id.* at 184:9-14. In December 2018, Apple also temporarily blocked Tumblr’s app from the Apple App Store “because Apple had detected child pornography on one single blog within the Tumblr ecosystem.” *Id.* at 184:15-20. Both actions posed a significant threat to Yahoo. Without a presence in the App Store, for example, no new mobile user could access Tumblr and view ads on Tumblr. *Id.* at 185:21-25. Yahoo’s investigations of violations of its TOS and attempts to remove child pornography are factors that “allowed Apple to let us relist the Tumblr app on the App Store.” *Id.* at 367:19-25. Zadig also testified that advertisers have boycotted other ISPs as a

result of child sex abuse material on those ISPs' services. *Id.* at 185:6-11.

Given Yahoo's independent business motivations for searching its services for child pornography, the instant case is much more like *Young*, in which the FedEx employee searched a package pursuant to an established company security policy. *Young*, 153 F.3d at 1080. In *Young*, the Ninth Circuit observed that FedEx had developed its security policies not to assist law enforcement, but rather to protect employee safety and to avoid tempting FedEx employees to steal packages. *Id.* at 1081. Because FedEx's security policy was enacted for its "own legitimate business purposes," the FedEx employee that searched the package did not act as an agent of the government. *Id.* Similarly, Yahoo investigated child pornography to keep its services safe and to maintain advertisement revenue, not out of any expectation of government reward or payment. Defendant identifies no case in which a court has extended *Walther* to such a search.

In sum, all circuits to address the issue—including the First, Fourth, Eighth, and Tenth Circuits—have concluded that an ISP is not a government agent when it searches a user's account pursuant to the ISP's own independent business motivation. All district courts to address the issue have rejected Defendant's arguments and reached the same conclusion, including in the cases that Defendant himself cites. Defendant has not cited a single case in which court concluded that an ISP like Yahoo acted as a government agent.

f. Defendant's Attempts to Distinguish this Case are Unpersuasive

Defendant contends that all of the aforementioned cases rejecting Defendant's arguments are inapplicable to his case for two primary reasons. First, Defendant contends that his case is unique because Yahoo identified Defendant as a buyer in the second supplemental report that Yahoo shared with NCMEC, and then only searched Defendant's account during Yahoo's third investigation—after NCMEC had shared Yahoo's second supplemental report with the FBI. Second, Defendant relies on numerous email communications between Yahoo's Sean Zadig and FBI agents. Neither argument is persuasive.

i. The Government Did Not Know that Yahoo was Going to Search Defendant's Email Account

Defendant’s first argument is unsupported by the record. In the instant case, Yahoo first listed Defendant as a buyer of child pornography in its second supplemental report to NCMEC in December 2014. *See* ECF No. 89, Ex. DD at 1574. That second supplemental report listed 267 seller accounts and 347 buyer accounts, for a total of 614 accounts. *Id.* at 1561–62, 1573.

Special Agent Yesensky testified that based on the information in the second supplemental report, which the FBI received from NCMEC, Defendant was not high on the FBI’s priority list. Tr. at 158:18-159:1. Yesensky was the sole agent assigned to OST for the duration of the FBI’s investigation into Philippines webcam pornography, and received only “piecemeal” assistance from other agents. *Id.* at 13:1-12. At most, Yesensky had assistance from two other law enforcement agents from time to time. *Id.* at 13:13-15. As a result, the FBI targeted seller accounts and priority buyers, or those buyers engaged in recent and actionable conduct. *Id.* at 27:18-25. Through that process, the FBI obtained 68 search warrants on seller accounts. *Id.* at 28:7-17. Processing and reviewing the returns from those 68 search warrants took the FBI approximately one year because Yesensky testified that “at most I had two other agents helping with the reviews.” *Id.* Accordingly, it is entirely reasonable that the FBI did not prioritize any investigation of Defendant—who was a buyer and one of 614 total accounts listed in the second supplemental report—in late 2014.

Zadig testified that Yahoo only decided to launch a third investigation in July 2015 after Yahoo learned that a Yahoo Messenger user in Texas had spent \$50,000 on child sex shows. Tr. at 213:20-25. Because most shows cost \$50, Yahoo was “concerned that that amount of money might indicate that there was an even greater webcam or sex trafficking problem on Yahoo Messenger” than Yahoo had thought after its second investigation, which had concluded in late 2014. *Id.* at 214:5-8.

During the third investigation, Yahoo determined that Defendant was connected to new seller accounts. *Id.* at 220:3-6. Yahoo then searched Defendant’s email account and discovered child pornography images and chats. *Id.* On November 30, 2015, Yahoo sent NCMEC CyberTip 7405007 on Defendant. ECF No. 28, Ex. D. Three months later, NCMEC sent CyberTip

7405007 to the FBI, which then determined that Defendant was a priority target and initiated the investigation that led to Defendant's arrest and indictment. ECF No. 85, Ex. D.

Defendant contends that the timeline of events raises the inference that the FBI and Yahoo were engaged in a "joint operation," such that after Yahoo identified Defendant as a buyer in the second supplemental report in 2014, the FBI "simply waited for Yahoo to conduct a warrantless search" of Defendant's account. Mot. at 21–22. However, the FBI was not simply waiting—Yesensky was processing and reviewing the returns for 68 search warrants on seller accounts (a process that took an entire year because Yesensky was assisted by at most two other agents from time to time) and identifying priority buyers out of the 347 accounts identified in the second supplemental report.

Moreover, there is no evidence that when Defendant's account was listed along with 613 other Yahoo accounts in the second supplemental report in December 2014, the government or Yahoo even knew that Yahoo would conduct a third investigation—let alone that the government encouraged Yahoo to conduct a third investigation.

Zadig testified that no law enforcement agent ever asked Yahoo to conduct further investigation of the subjects listed in the second supplemental report. *Id.* at 212:19-213:3. In fact, Zadig only informed Yesensky of the existence of a third investigation in a July 23, 2015 email that Zadig sent after Yahoo initiated the investigation:

On a related note – we're working on a new Philippines case. No idea how large it will be yet, we discovered it yesterday on some proactive scanning we're doing. Will keep you informed. We do see some overlap with some of the buyers, but a different set of sellers. Lots of travelers again. Won't be able to share anything until we've finished our investigation, but wanted to give you a heads up.

RR at 1649. Thus, Zadig told the FBI that Yahoo could not share any information about Yahoo's investigation—except for the investigation's existence—until after Yahoo finished its investigation. In sum, there is no evidence that the FBI knew that Yahoo was investigating Defendant or that Yahoo would search Defendant's Yahoo account.

ii. Zadig's Email Communications Do Not Prove that Yahoo was an Instrument or Agent of the Government

Finally, Defendant focuses on Zadig’s email communications with FBI agents, primarily Yesensky. However, none of those communications show that the government knew that Yahoo was going to search Defendant’s account, or indicate that Yahoo lacked an independent business motivation for its investigations of child pornography on its services. The emails fall into four broad categories: (1) the exchange of post-indictment, public information about case outcomes; (2) Yahoo’s attempts to prevent active sexual abuse or the murder of children; (3) exchanges related to the service of legal process on Yahoo; and (4) introductions to individuals from other private companies or law enforcement involved in investigating child pornography. The Court addresses each in turn.

a. Exchanges of Post-Indictment, Public Information About Case Outcomes

First, Yahoo occasionally sought information from the FBI about child pornography investigations or prosecutions. In response, the FBI shared only publicly available information about indicted cases.

For example, on June 13, 2016, Zadig emailed FBI Special Agent Peter Kaupp to ask for an update on a search warrant that the FBI had served on Yahoo: “I wanted to follow up with you to see if you have any updates on the investigation. Has any action been taken, or have you decided not to proceed?” Ex. SS at 2098. Kaupp wrote that he could not share any information about a pending investigation: “Hi Sean. The investigation is pending. Unfortunately I cannot share details. Will let you know when I can.” *Id.* Eight months later, in February 2017, Kaupp emailed Zadig to advise him that the subject had been arrested. *Id.* at 2097. Zadig asked for a mugshot, but Kaupp again rejected Zadig’s request and reminded him that “my office is very strict about releasing information, including photos to the public. I will continue to keep you posted on any/all plea, trial, and/or sentencing dates.” *Id.* at 2096.

Accordingly, the FBI provided Yahoo only with public information after indictment, and refused to share with Yahoo any non-public details of the FBI’s investigations or prosecutions. *See also* ECF No. 89, Ex. C at 733 (Special Agent Ann Trombetta informing Zadig of Defendant’s indictment); Ex. RR at 1685 (Yesensky sending Yahoo and Xoom public media reports about the

1 FBI's OST investigation).

2 Yahoo seeks such information primarily to provide feedback and closure to Yahoo's
3 employees who review and report child pornography. Zadig testified that these employees
4 experience trauma from viewing such content:

5 Primarily it is because we have found that the practice of – our employees who deal
6 with this content, that is, child exploitation and sexual abuse content, it's very
7 emotionally difficult to be exposed to that type of content. In fact, it actually,
8 essentially the brain, according to our wellness specialists that we bring in,
9 experiences trauma when employees or people are exposed to that type of content.

10 Tr. at 254:21-255:4. Accordingly, counselors recommend that Yahoo "obtain feedback to provide
11 both closure to the people who are exposed to this content, so that's my team, the ECIT team, as
12 well as engineers who build the tools across the company, and the front-line reviewers on our
13 moderation team." *Id.* at 255:9-13. When available, mugshots show "that there's a real person
14 behind the accounts that they're interacting with, which is kind of sobering." *Id.* at 284:15-19.

15 Another reason Yahoo seeks information about prosecutions is to generate management
16 support for ECIT's work because child safety reporting does not generate revenue for Yahoo. *Id.*
17 at 256:4-20. Thus, ECIT shares positive outcomes like child rescues and arrests to generate
18 management support for its work. *Id.* Zadig testified that Yahoo management was "frankly,
19 shocked that this type of conduct was happening on the platforms that they operated," and was
20 supportive of the investigations to rid Yahoo's platforms of this conduct. *Id.* at 262:13-22.

21 These two Yahoo motivations are memorialized in Zadig's July 6, 2016 email to Rab Seip,
22 an agent with the Australian Federal Police ("AFP"). In the email, Zadig informs Seip that
23 information about arrests and charges justifies ECIT's efforts to Yahoo's management and "is a
24 huge morale boost for our front-line reviewers who spend day in and day out looking at child
25 abuse images to report them." Specifically, Zadig wrote:

26 It greatly helps us when we learn of arrests, charges, and the like from our case
27 referrals – it justifies our efforts to our management, and the news is a huge morale
28 boost for our front-line reviewers who spend day in and day out looking at child
abuse images to report them. We do not talk about these successes outside of Yahoo,
as we try to avoid publicity at all costs.

Would you be able to provide feedback on our prior referrals and on cases going forward? This feedback might be as simple as “subject arrested on June 1, 2016, and two children rescued” or “case closed due to the lack of evidence.” Having this relationship would be productive for both sides.

Ex. RR at 1708–09.

Yahoo’s interest in learning about the status of investigations and the success of prosecutions does not indicate that Yahoo had a law enforcement purpose. Rather, it is entirely consistent with Yahoo’s business motivations to rid its services of child pornography, and to give closure to and encourage its employees involved in that endeavor.

b. Yahoo’s Attempts to Prevent Actual Sexual Abuse or the Murder of Children

Second, on rare occasions, Yahoo reached out to the FBI to alert the FBI of individual CyberTips that Yahoo had already sent to NCMEC. Zadig testified that Yahoo advised the FBI of these egregious CyberTips because “of what we believed to be imminent child abuse that would happen without – if we didn’t notify law enforcement, this child abuse would occur.” Tr. at 268:11-17. Zadig never emailed the FBI information that was not in the CyberTips, nor is there evidence that the FBI encouraged Zadig to highlight any CyberTips.

For example, on January 16, 2016, Zadig told Yesensky about a CyberTip that Yahoo had submitted to NCMEC that concerned a subject involved in the murder of children: “When you’re back in the office, please take a look at CT [redacted]. Apparent German who lives in Singapore and who travels to PH frequently, planning another trip in Feb.” RR at 1737. Zadig testified that the CyberTip was extremely concerning to Yahoo:

He was – he was a German banker residing in Singapore for Deutsche Bank. But then he, on the side, operated a sex tourism business, and one of the services that this business offered was what’s called snuff, or essentially a murder, for sexual gratification, of children. So we were extremely concerned about the snuff conversations and wanted to make sure that the FBI had a chance to look at that ahead of our meeting.

Tr. at 348:14-21. Zadig testified that Yahoo highlighted this and other egregious CyberTips because Yahoo had not yet scheduled a meeting to discuss CyberTips with the FBI at the time, and Yahoo was concerned that “in essence child abuse would occur in that

intermediate time.” *Id.* at 347:14-17.

Similarly, on January 20, 2016, Zadig emailed Yesensky and a Thai policer officer to notify them of a CyberTip about a “missionary who does a lot of work with orphans, and supposedly received a commendation from the White House.” Ex. RR at 1645. The CyberTip indicated that the missionary might be traveling to Thailand to meet underage girls for sex:

Our investigation revealed that he possesses CSAI and may also be meeting underage girls in Thailand for sex. Given the level of access he likely has to vulnerable children, we wanted to be sure that you both were aware of this. Feel free to let Jeff Zingler or myself know if you have any questions or have difficulty downloading the supplemental information from NCMEC.

Id. at 1645. Zadig testified that his email about sexual abuse of children in Thailand was “not connected to the Philippines webcam investigation.” Tr. at 269:21-23.¹ Rather, Zadig testified that he emailed Yesensky because Zadig knew that Yesensky had done work in Thailand unrelated to Philippines webcam child pornography, and Zadig “wanted to make sure he was aware so he could try to get the proper resources directed to this.” *Id.* at 270:8-20. Zadig testified that all of the information in the email was included in the CyberTip that Yahoo had submitted to NCMEC. *Id.* at 272:21-23.

Ultimately, Defendant has not shown that Yahoo highlighted CyberTips out of a law enforcement purpose. Rather, Yahoo wished to prevent the imminent sexual abuse or murder of children facilitated by Yahoo’s own services. Such a desire does not transform Yahoo into a government agent. Even a dual motive to “assist the police” does not override Yahoo’s independent business motivation to eradicate child sexual abuse from its services or Yahoo’s duty as a private citizen to report possible criminal activity. *Cleaveland*, 38 F.3d at 1094 (holding that a private citizen’s “legitimate, independent motivation” for a search is “not negated by any dual

¹ The government disclosed this email as part of its disclosure of all communications between Yesensky and Zadig, which included discovery beyond Yahoo’s Philippines webcam investigation and beyond the FBI’s OST. Tr. at 269:21-272:21. That the government disclosed emails not even related to the Philippines webcam investigation in this case further reinforces the Court’s conclusion in its order denying Defendant’s fourth motion to compel that Defendant was able to obtain extensive discovery to support his motion to suppress. Defendant submitted hundreds of pages of emails with his motion to suppress.

1 motive to detect or prevent crime or assist the police”); *see also Walther*, 652 F.2d at 793 (stating
2 that the Ninth Circuit did not “diminish the duty of any private citizen to report possible criminal
3 activity”).

4 c. Exchanges Regarding Service of Legal Process

5 Third, Zadig communicated with FBI agents about how to serve legal process on Yahoo.
6 At no point did Zadig provide information about user accounts outside of legal process, nor did the
7 FBI request any information outside of legal process. Tr. at 213:4-7.

8 For example, Zadig ensured that FBI agents understood Yahoo’s policy for when Yahoo
9 would notify a user of legal process served on the user’s account. Generally, in child abuse
10 investigations, Yahoo will “provide a voluntary delay of notification” upon service of legal
11 process. Tr. at 293:8-10. On March 2, 2015, FBI Special Agent Caliope Bletsis emailed Zadig to
12 ask why Yahoo was not withholding notification to a user. Ex. SS at 2071–72. Zadig explained
13 Yahoo’s user notification policy, advised the agent to specify that the warrant was for a child
14 abuse investigation, and stated that the “best practice for your team going forward might be if
15 you’re going before a judge anyhow to get a warrant, get the non-disclosure order while you are in
16 front of the magistrate.” *Id.* at 2071. Thus, Zadig simply informed Bletsis of Yahoo’s policy and
17 suggested that Bletsis receive a court order. Bletsis did not request, nor did Yahoo provide, any
18 information about the user account other than how to serve legal process.

19 Moreover, Zadig testified that Yahoo had an independent reason for wanting to ensure that
20 the FBI understood Yahoo’s user notification policy because a user notification could tip off an
21 abuser to “take actions to evade capture or prevent the child from being rescued or other bad
22 things from happening.” Tr. at 340:18-23. Moreover, if the user evaded capture, the user could
23 continue to buy or sell child sexual abuse materials on Yahoo’s services.

24 Occasionally, Zadig asked Yesensky whether Yesensky could assist foreign law
25 enforcement officers with service of legal process on Yahoo. However, Yesensky testified that he
26 never felt compelled to follow Zadig’s suggestions for how the FBI could assist foreign law
27 enforcement with service of legal process. Tr. at 60:21-61:1. Moreover, Zadig made such

1 inquiries because Yahoo believed that “expediency” was essential due to imminent or ongoing
2 child abuse facilitated by Yahoo’s services. *Id.* at 280:12-15.

3 For example, on November 16, 2016, Zadig emailed Yesensky:

4 I got a ping from German BKA [German federal police] regarding [redacted]. They
5 are working on that case they are asking questions about how to obtain account
6 contents. Unfortunately, they will need to serve Ireland with a MLAT to get the
contents.

7 Would the FBI be able to obtain with a SQ the accounts that [redacted] used and send
8 them to the Germans on a LE-to-LE basis? The four accounts in question are
[redacted].

9 Not sure if this is something that can be done, but given that [redacted] appeared to
10 be communicating with [redacted] perhaps that can be nexus for FBI to do the SW.”

11 RR at 1773.

12 Thus, Zadig’s email concerned the German federal police’s investigation of a German
13 citizen. The email did not involve or aid the FBI’s investigation of any individual in the United
14 States, let alone involve or aid the FBI’s investigation of Defendant. By November 2016, the FBI
15 had already obtained and executed a search warrant on Defendant’s Yahoo account. ECF No. 28,
16 Ex. A. Accordingly, the email is not relevant to Yahoo’s motivation for searching Defendant’s
17 email account.

18 Moreover, Zadig’s email is consistent with his role as a liaison for service of legal process
19 on Yahoo. Zadig testified that he asked Yesensky about whether the FBI could seek a search
20 warrant (or “SW”) because the mutual legal assistance treaty (“MLAT”) process “is very time
21 intensive.” Tr. at 280:6-10. Yahoo was “concerned that this individual, as I mentioned, was
22 operating an orphanage and was believed to be abusing many children in his care, and we thought
23 that expediency would be helpful here.” *Id.* at 280:12-15. Accordingly, Zadig’s inquiry is
24 consistent with Yahoo’s independent business motivation to eradicate child pornography from its
25 services, Zadig’s role as a liaison for service of legal process on Yahoo, and Yahoo’s duty as a
26 private citizen to report child sexual abuse. Moreover, the German police ultimately obtained an
27 MLAT, and did not receive information through the FBI. *Id.* at 281:9-13.

d. Introductions to Others Combating Child Pornography

Fourth, Zadig occasionally introduced Yesensky to others in private companies or in law enforcement combating child pornography. Defendant makes much of one such email in which Zadig referred to a “common goal.” Ex. RR at 1650. However, the reference to a “common goal” suggests only that Yahoo’s independent business motivation to remove child pornography from its services, Yahoo’s duty as a private citizen to report child sexual abuse, and the FBI’s law enforcement interest in prosecuting violations of child pornography statutes overlap.

On June 11, 2015, Zadig wrote an email to introduce Yesensky to Jeff Jones, an investigator at the money transfer service Western Union. Ex. RR at 1650. Zadig also referred to a common goal: “SA Yesensky and I were discussing today some approaches to combating child exploitation (specifically webcam cases) and opportunities for all of us to work towards the common goal.” *Id.* Zadig testified that “the common goal I refer to is the essential – essentially the removal or the stopping of online platforms being used for the sale of child sexual abuse material.” Tr. at 275:10-12.

As for the FBI, Yesensky testified that the FBI’s goal is “investigating alleged conduct for violations of U.S. law,” not ensuring that Yahoo’s services remain clean of child pornography. *Id.* at 136:7-24. Yesensky understood Zadig to be referring to a common goal—as the email states—of “combating child exploitation.” *Id.* at 57:15-18. Thus, the email does not indicate that the FBI deputized Yahoo as a government agent. Rather, because Yahoo wished to eradicate child pornography from its services and to prevent child sexual abuse, and the FBI wished to prosecute child pornography crimes, both entities were interested in the broader common goal of combating webcam child pornography.

Regardless, even if Zadig desired to assist the FBI, a private party’s “legitimate, independent motivation” to further its own business interests is “not negated by any dual motive to detect or prevent crime or assist the police.” *Cleaveland*, 38 F.3d at 1094. A private party that discovers illegal conduct is not prevented from disclosing such conduct to law enforcement. *See also Walther*, 652 F.2d at 793 (“We do not by this opinion diminish the duty of any private citizen

to report possible criminal activity.”). Unlike in *Walther*, Defendant has not shown that Yahoo or Zadig were solely motivated by any promise of government reward. To the contrary, Yahoo initiated its investigations of Philippines webcam child pornography for its own business purposes and never took direction from the government with respect to any of Yahoo’s investigations.

Accordingly, for all of the foregoing reasons, the Court concludes that Yahoo was not acting as a government agent subject to the Fourth Amendment when Yahoo searched Defendant’s email account. As a result, Yahoo’s search could not and thus did not violate the Fourth Amendment.

2. Good Faith Exception

Furthermore, even if Defendant had shown that Yahoo’s private search was government action in violation of the Fourth Amendment, the Court would conclude that the good faith exception to the exclusionary rule precludes suppression. Pursuant to the good faith exception, the Court may suppress evidence obtained in violation of the Fourth Amendment “only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment.” *Illinois v. Krull*, 480 U.S. 340, 348–49 (1987).

Defendant has not identified a single case in which a court has determined that an ISP’s private search of its own user’s account constituted government action. By contrast, every court to consider the question—including the First, Fourth, Eighth, and Tenth Circuits—has concluded that an ISP’s search of its own user’s account does not implicate the Fourth Amendment. Accordingly, no law enforcement officer had knowledge, or may properly be charged with knowledge, that Yahoo’s search of Defendant’s email account was unconstitutional. *Krull*, 480 U.S. at 348 (holding that suppression is warranted “only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment”). Thus, the good faith exception to the exclusionary rule applies and precludes suppression of the eight images found in Defendant’s email account.

Indeed, in *Viramontes*, the district court also held that the good faith exception would

preclude suppression of the fruits of Dropbox’s search of Viramontes’s account because no government official would have any reason to believe that Dropbox’s search was unconstitutional. ECF No. 62 at 17–18; *see also United States v. Korte*, 918 F.3d 750, 758 (9th Cir. 2019) (holding that the good faith exception applies where the government does not have “any reason to doubt” the constitutionality of a search). Therefore, even if Yahoo’s private search violated the Fourth Amendment, the good faith exception to the exclusionary rule applies and precludes suppression of the eight images that Yahoo found in Defendant’s email account.

B. *Franks* Motion to Suppress

Lastly, the Court discusses Defendant’s motion to suppress all evidence pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). Defendant contends that Special Agent Trombetta’s affidavit submitted with the FBI’s 2016 search warrant on Defendant’s Yahoo account intentionally omitted material information. Specifically, Defendant contends that Trombetta’s affidavit failed to disclose the details of Yahoo’s 2015 search of Defendant’s email account, which Defendant argues would have alerted the magistrate judge to the illegality of Yahoo’s search. ECF No. 184 at 4–5. Defendant requests an evidentiary hearing under *Franks*. However, because Defendant has failed to show that Yahoo’s private search of Defendant’s email account was illegal, the Court finds that an evidentiary hearing is not warranted and concludes that Defendant’s *Franks* motion also fails.

“In *Franks*, the [U.S.] Supreme Court held that a defendant could challenge a facially valid affidavit by making a substantial preliminary showing that (1) the affidavit contains intentionally or recklessly false statements, and (2) the affidavit purged of its falsities would not be sufficient to support a finding of probable cause.” *United States v. Stanert*, 762 F.2d 775, 780 (9th Cir. 1985) (internal quotation marks omitted). If the defendant makes this substantial preliminary showing, “the Fourth Amendment requires that a hearing be held at the defendant’s request.” *Franks*, 438 U.S. at 156. There is “a presumption of validity” for information in a search warrant affidavit. *Id.* at 171. As a result, the defendant’s allegations of falsity must be “more than conclusory,” and must be “accompanied by an offer of proof” such as “[a]ffidavits or sworn or otherwise reliable

statements of witnesses.” *Id.*

The Ninth Circuit has “recognized that an affiant can mislead a magistrate ‘[b]y reporting less than the total story, [thereby] . . . manipul[at]ing the inferences a magistrate will draw.’” *United States v. Perkins*, 850 F.3d 1109, 1117–18 (9th Cir. 2017) (alterations in original) (quoting *Stanert*, 762 F.2d at 781). For example, in *Perkins*, the affiant “presented a skewed version of events and overstated the incriminating nature of the images.” *Id.* at 1118.

In the instant case, Defendant has failed to show that the affidavit supporting the FBI’s search warrant for Defendant’s Yahoo account would not be sufficient even if the affidavit included the omitted information. *See Stanert*, 762 F.2d at 782; *see also United States v. Shayota*, 186 F. Supp. 3d 1052, 1062 (N.D. Cal. 2016) (denying motion to suppress pursuant to *Franks* where omitted information would not have affected the issuance of the search warrant). Moreover, Defendant has not made a substantial showing that any omission of information about Yahoo’s 2015 search of Defendant’s email account was intentional or reckless.

As relevant here, Trombetta’s affidavit explained that (1) Yahoo conducted investigations of child pornography on its platform after Xoom alerted Yahoo “that a number of Yahoo accounts were engaged in the sale of child exploitation material; (2) Yahoo sent NCMEC a CyberTip on Defendant after Yahoo discovered eight child pornography images in Defendant’s email account; (3) Trombetta had reviewed the eight images in the CyberTip and determined that all of them “appeared to be photographs of two girls who appear to be under twelve years old, performing sexual acts on themselves.” ECF No. 28, Ex. A at ¶¶ 35–40. Those statements are plainly sufficient to establish probable cause that Defendant knowingly possessed a visual depiction with the intent to view a minor engaging in sexually explicit conduct and that Defendant possessed child pornography. 18 U.S.C. §§ 2252(a)(4)(B), 2252A(a)(5)(B).

The only allegedly omitted information—about Yahoo’s series of investigations and the FBI’s OST investigations—was the subject of Defendant’s motion to suppress pursuant to *Walther*. As set forth at length above, Yahoo’s private search of Defendant’s account did not violate the Fourth Amendment. Moreover, no court has found that an ISP’s private search of its

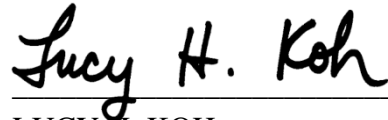
own user's account for the ISP's own independent business reasons violates the Fourth Amendment. Accordingly, even if Trombetta had disclosed additional details of Yahoo's investigations and the FBI's investigations, the affidavit would not have alerted the magistrate judge to any illegality and the affidavit would remain sufficient to support probable cause. Therefore, the Court denies Defendant's *Franks* motion to suppress.

IV. CONCLUSION

For the foregoing reasons, the Court DENIES Defendant's motions to suppress.

IT IS SO ORDERED.

Dated: December 10, 2019



LUCY H. KOH
United States District Judge